IN THE CLAIMS:

1. (currently amended) A method for securing network-connected resources, the method comprising:

at a first network-connected node, receiving an unencrypted electronically formatted job;

receiving CK, a symmetrical encryption key (K) encrypted using an asymmetrical encryption public key (pubK);

receiving CH, a hash (H) of the job, further encrypted using K;

receiving a selection command for a particular one of a plurality of encrypted resources;

decrypting CK using an asymmetrical encryption private key (privK), corresponding to pubK, to recover K;

hashing the job, generating H';

using K to validate CH;

in response to validating CH, decrypting an encrypted resource using K; [[and,]]

using the decrypted resource to process the job;

wherein receiving a selection command for a particular one of a plurality of encrypted resources includes receiving CK_i, where $1 \le i \le m$; and,

wherein decrypting the selected resource in response to the encrypted resource selection command includes decrypting CK_i to recover one of symmetrical encryption keys K_1 through K_m, where K_1 through K_m correspond to encrypted resources CR_1 through CR_m.

2. (currently amended) The method of claim 1 ~~wherein~~ using K_i to validate CH_i as follows ~~includes~~:

encrypting H' using K_i, obtaining CH_i'; and,

matching CH_i to CH_i'.

3. (currently amended) The method of claim 1 ~~wherein~~ using K_i to validate CH_i as follows ~~includes~~:

decrypting CH_i using K_i, generating H; and,

comparing H to H'.

4. (currently amended) The method of claim 1 further comprising:

prior to receiving the job, CK_i, and CH_i, receiving the encrypted resource; and,

storing the encrypted resource.

5. (currently amended) The method of claim 4 further comprising:

installing pubK [[,]] and privK upon initialization.

6. (previously presented) The method of claim 1 wherein receiving the unencrypted electronically formatted job includes receiving a print job in a format selected from the group including text and image formats.

7. (original) The method of claim 4 wherein storing the encrypted resource includes storing an encrypted font resource; and,

wherein using the decrypted resource to process the job includes printing a print job using the decrypted fonts.

8. (original) The method of claim 7 wherein storing the encrypted font resource includes storing resources selected from the group including a logo, personal signature image, and glyph.

9. (original) The method of claim 4 wherein receiving the encrypted resource includes receiving the encrypted resource in a format selected from the group including hypertext transport protocol (http) and file transport protocol (FTP).

10. (original) The method of claim 1 further comprising:

at a second network-connected node, generating the job;
encrypting K_i with pubK, generating CK_i;
hashing the job, generating H;
encrypting H using K_i, generating CH_i; and,
sending the job, CK_i, and CH_i to the first node for job processing.

11-12. canceled

13. (currently amended) The method of claim 1 wherein receiving the unencrypted electronically formatted job includes receiving the job at network-connected node N[[*i*]]$\underline{k}$, where 1≤ [[*i*]]$\underline{k}$ ≤*n*;

wherein receiving $CK_{\underline{i}}$ includes N_i receiving $CK_{i\underline{k}}$, where $CK_{i\underline{k}}$ is generated by encrypting K_i using corresponding asymmetrical encryption public key pubK$[[_i]]_{\underline{k}}$; and,

wherein decrypting CK includes N_i decrypting $CK_{i\underline{k}}$ using corresponding asymmetrical encryption private key privK$[[_i]]_{\underline{k}}$, to recover $K_{\underline{i}}$.

14. (currently amended) The method of claim 1 wherein receiving the unencrypted electronically formatted job includes receiving the job at network-connected node N$[[_i]]_{\underline{k}}$, where 1≤ $[[i]]\underline{k}$ $\leq n$;

wherein receiving CK includes N_i receiving $CK_{i\underline{k}}$, corresponding to symmetrical encryption key $K_{i\underline{k}}$, encrypted using pubK$[[_i]]_{\underline{k}}$;

wherein receiving CH includes N_i receiving $CH_{i\underline{k}}$, a hash of the job encrypted using corresponding symmetrical encryption key $K_{i\underline{k}}$; and,

wherein decrypting CK includes N_i decrypting $CK_{i\underline{k}}$ using asymmetrical encryption private key privK$[[_i]]_{\underline{k}}$, to recover corresponding symmetrical encryption key $K_{i\underline{k}}$.

15. (currently amended) The method of claim 14 wherein using K to validate CH includes:

N$[[_i]]_{\underline{k}}$ encrypting H' using symmetrical encryption key $K_{i\underline{k}}$, obtaining $CH_{i\underline{k}}$';

N$[[_i]]$ matching $CH_{i\underline{k}}$ to corresponding $CH_{i\underline{k}}$'; and, wherein decrypting an encrypted resource using K includes N[[i]] decrypting the encrypted resource using symmetrical encryption key $K_{i\underline{k}}$.

16. (currently amended) The method of claim 14 wherein using K to validate CH includes:

N[[i]] decrypting $CH_{i\underline{k}}$ using symmetrical encryption key $K_{i\underline{k}}$, obtaining H;

N_i comparing H to H'; and,

wherein decrypting an encrypted resource using K includes N_i decrypting the encrypted resource using symmetrical encryption key $K_{i\underline{k}}$.

17. (currently amended) A method for accessing network-connected processing resources, the method comprising:

at a second node, generating an unencrypted electronically formatted job;

encrypting a symmetrical encryption key K with an asymmetrical encryption key (pubK), generating CK;

hashing the job generating H;

encrypting H using K, generating CH;

sending the job, CK, [[and]] CH and a selection command for a particular one of a plurality of encrypted resources to a first network-connected node; and,

processing the job at the first node using a K encrypted resource;

wherein encrypting the symmetrical encryption key K with an asymmetrical encryption key (pubK), generating CK, includes encrypting K_i, where K_1 through K_m correspond to encrypted resources CR_1 through CR_m, with pubK to generate CK_i; and,

wherein sending the selection command for a particular one of a plurality of encrypted resources includes sending CK_i.

18. (currently amended) A system for using secure network-connected resources, the system comprising:

a first device including:

a network-connected port for receiving an unencrypted electronically formatted job, for receiving CK, a symmetrical encryption key (K) encrypted using an asymmetrical encryption public key (pubK), and for receiving CH, a hash (H) of the job, further encrypted using K;

a hash unit having an interface to accept the job and to supply a hash of the job (H');

a memory having an interface to supply an asymmetrical encryption private key ($privK_i$), corresponding to $pubK_i$, and an encrypted resource;

a security unit having an interface to authorize access to the encrypted resource in memory, in response to validating CH_i; [[and,]]

a processing unit having an interface to accept the job and a decrypted resource, and to supply a job processed using the decrypted resource;

wherein the first device network-connected port receives a encrypted resource selection command; and, wherein the decryption unit decrypts CK_i, where $1 \leq i \leq m$, to recover one of symmetrical encryption keys K_1 through K_m, where K_1 through K_m correspond to encrypted resources CR_1 through CR_m.

19. (currently amended) The system of claim 18 further comprising:

~~a decrypting unit having an interface to accept CK and privK, to generate K in response to decrypting CK using privK, to decrypt the encrypted resource from memory using K, and supply the decrypted resource;~~

an encryption unit having an interface to accept H' and K_i, and supply CH_i' in response to using K_i to encrypt H'; and,

wherein the security unit accepts CH_i and CH_i' and validates CH_i by matching CH_i to CH_i'.

20. (currently amended) The system of claim 18 ~~further comprising:~~

~~a decrypting unit having an interface to accept CH, CK, and privK, to generate K in response to decrypting CK using privK, to supply H in response to decrypting CH using K, and supply the decrypted resource; and,~~

wherein the security unit accepts H and H' and validates CH_i by matching H to H'.

21. (original) The system of claim 18 wherein the network-connected port receives the encrypted resource for storage in the memory.

22. (original) The system of claim 18 wherein the memory is a read only memory (ROM) for accepting and storing privK upon device initialization.

23. (original) The system of claim 18 wherein the first device is a printer; and,

wherein the network-connected port receives a print job in a format selected from the group including text and image formats.

24. (original) The system of claim 23 wherein the memory stores encrypted font resources; and,

wherein the processing unit is a print engine that supplies a job printed using the decrypted fonts.

25. (original) The system of claim 24 wherein the memory stores encrypted font resources selected from the group including a logo, personal signature image, and glyph.

26. (original) The system of claim 21 wherein the network-connected port receives an encrypted resource for storage in a format selected from the group including hypertext transport protocol (http) and file transport protocol (FTP).

27. (currently amended) The system of claim 18 further comprising:

a second device including:

a processor to supply a job;

a hash unit having an interface to accept the job and to supply a hash of the job (H);

an encryption unit having an interface to accept H, to supply CK_i, the encryption of symmetrical encryption key K_i using $pubK_i$, and CH_i, the encryption of H using K_i; and,

a network-connected port for transmitting the job, CK_i, and CH_i to the first device for job processing.

28-29. canceled

30. (currently amended) The system of claim 18 further comprising:

a plurality of devices ~~N_i, where $1\leq i \leq n$~~, each receiving the unencrypted electronically formatted job at a network-connected port, along with CK_i, where CK_i is generated by encrypting K_i using an ~~corresponding~~ asymmetrical encryption public key pubK[[i]] uniquely associated with each device; and,

wherein each device decryption unit decrypts CK_i using corresponding asymmetrical encryption private key $privK_i$, to recover K_i.

31. (currently amended) The method of claim 18 further comprising:

a plurality of devices ~~N_i, where $1\leq i \leq n$,~~ each receiving the unencrypted electronically formatted job at a network-connected port, along with CK_i, where CK_i is generated by encrypting K_i, uniquely associated with each device, using an ~~corresponding~~ asymmetrical encryption public key pubK[[i]], uniquely associated with each device, and CH_i, a hash of the job encrypted using corresponding symmetrical encryption key K_i~~; and,~~

~~wherein each device includes a decryption unit for decrypting CK_i using asymmetrical encryption private key $privK_i$, to recover corresponding symmetrical encryption key K_i, for the decryption of the encrypted resource~~.

32-33. canceled

34. (currently amended) A system for accessing network-connected processing resources, the system comprising:

a second device including:

a processor to supply an unencrypted job;

a hash unit having an interface to accept the job and to supply a hash of the job (H);

an encryption unit having an interface to accept H_i, to supply CK_i, the encryption of symmetrical encryption key K_i, where $1 \leq i \leq n$, using pubK, [[and]] CH_i, , where K_1 through K_m correspond to encrypted resources CR_1 through CR_m, the encryption of H using K_i, and an encrypted resource selection command; and,

a network-connected port for transmitting the job, CK_i, and CH_i to a first device for job processing.